



## **Accelerating The Application Vulnerability Scanning Process with Qualys WAS and Azure DevOps**



Celestica™

## A Global Leader in Innovative End-to-End Product Lifecycle Solutions

- Focused on enabling the world's leading technology brands
- Tailoring customer-centric solutions for the markets we serve
- Operating a global network of sites with specialized Centers of Excellence

**\$6.6 billion**  
in 2018 revenue

**38 locations**  
in 14 countries  
Headquartered  
in North America

**28,000**  
employees  
worldwide

**Over 100**  
customers  
across multiple  
markets





## The Markets We Serve

Advanced  
Technology  
Solutions

Aerospace  
& Defense



Smart Energy



Industrial



HealthTech



Capital Equipment



Connectivity &  
Cloud Solutions

Service Provider Solutions



Enterprise



# Global Footprint

Celestica locations across the globe



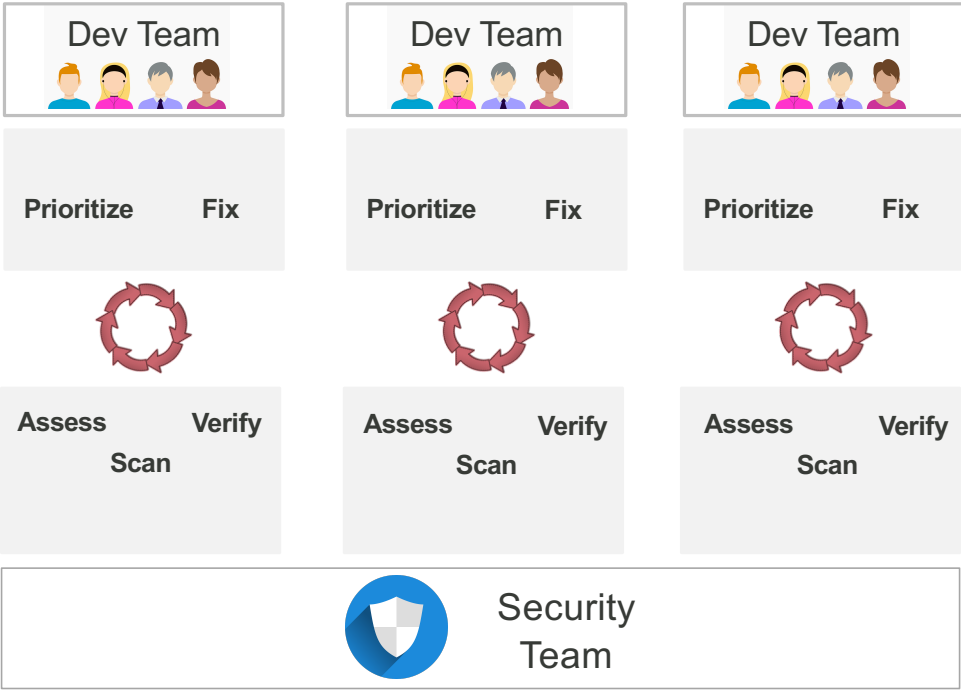
- Central, Regional, Site and Cloud Data Centers
- 100's of Applications
- Globally Distributed Development Teams
- 100's of Developers, 1000's of Engineers



## The Challenge

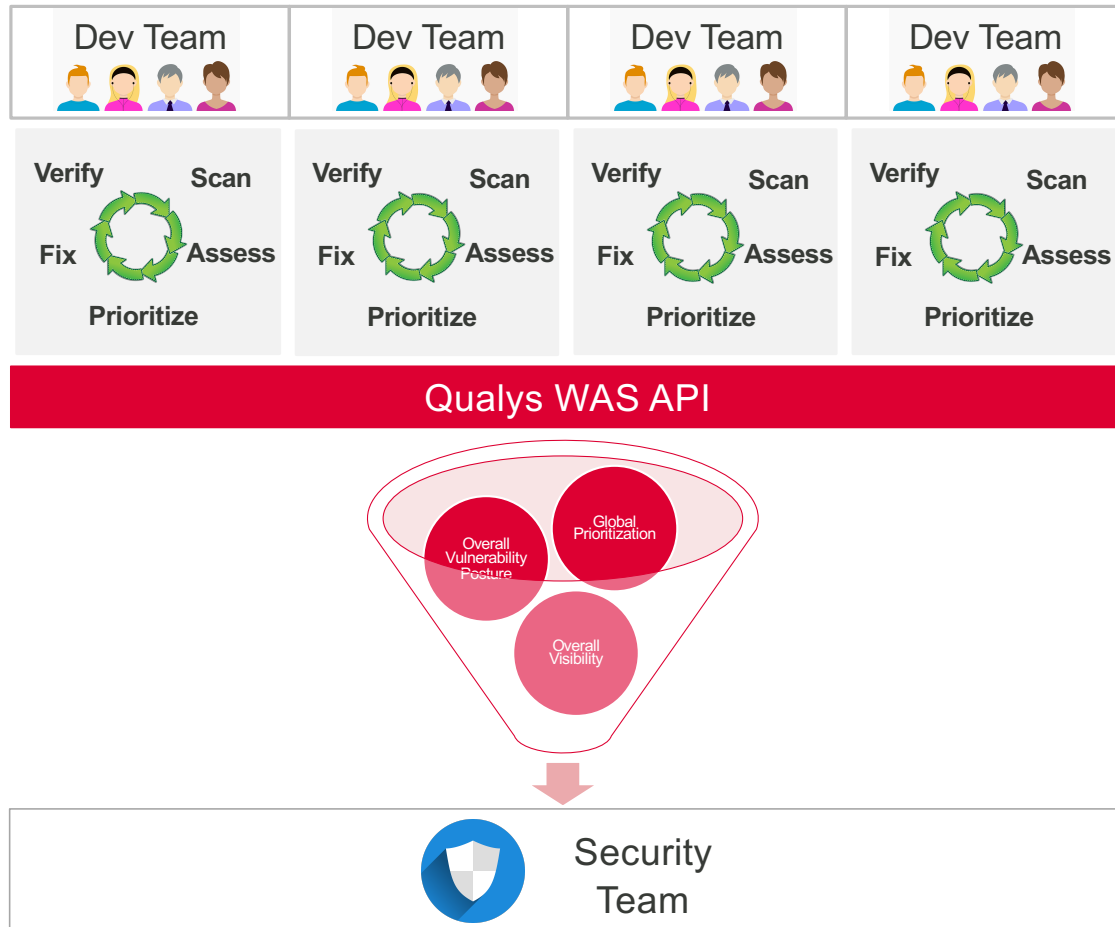


Before Qualys WAS



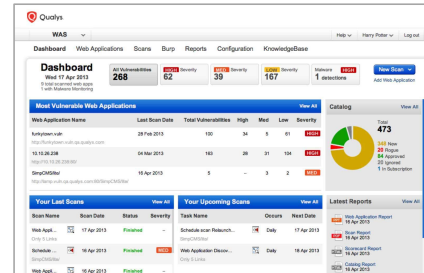


## After Qualys WAS



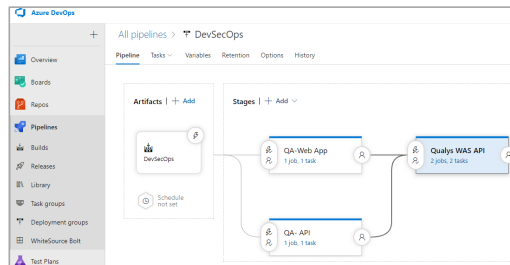
## Speed up the process

Triggers scan



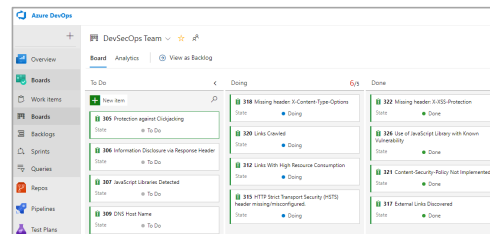
Qualys WAS

Pulls findings



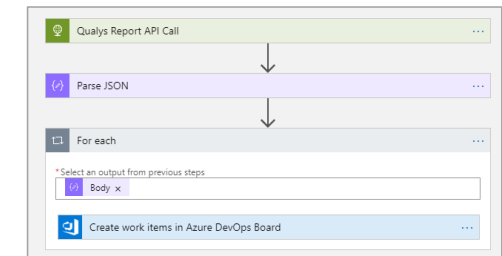
Azure DevOps Pipeline

Remediated Items ready to build



Azure DevOps  
Boards / Work Items

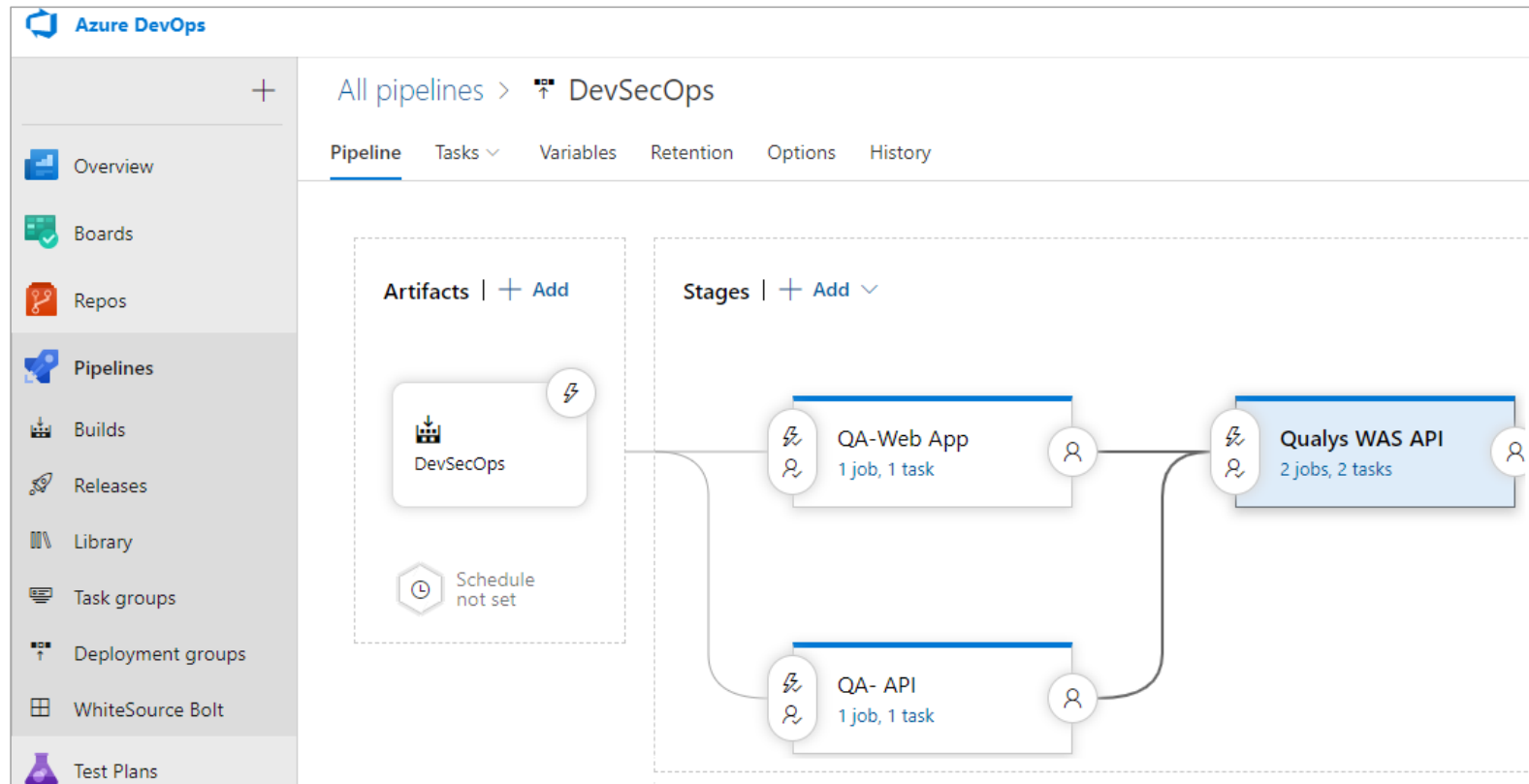
Converts findings to work items



Azure LogicApp



# Azure DevOps Pipeline



## Azure DevOps Board

**Azure DevOps**

DevSecOps Team

Board Analytics View as Backlog

To Do	Doing 6/5	Done
<b>305</b> Protection against Clickjacking State ● To Do	<b>318</b> Missing header: X-Content-Type-Options State ● Doing	<b>322</b> Missing header: X-XSS-Protection State ● Done
<b>306</b> Information Disclosure via Response Header State ● To Do	<b>320</b> Links Crawled State ● Doing	<b>326</b> Use of JavaScript Library with Known Vulnerability State ● Done
<b>307</b> JavaScript Libraries Detected State ● To Do	<b>312</b> Links With High Resource Consumption State ● Doing	<b>321</b> Content-Security-Policy Not Implemented State ● Done
<b>309</b> DNS Host Name State ● To Do	<b>315</b> HTTP Strict Transport Security (HSTS) header missing/misconfigured. State ● Doing	<b>317</b> External Links Discovered State ● Done



## In Conclusion

- 3x – 5x turn around time reduction on vulnerability fixes
- Expanded coverage of application security program
- Progress towards “continuous compliance”
- Continuous training for software engineers
- The journey continues...

